California Secretary of State
Consultant's Report on:

HART INTERCIVIC

SYSTEM 6.1:
Ballot Now, version 3.2.4
BOSS, version 4.2.13
Rally, version 2.2.4
Tally, version 4.2.8
SERVO, version 4.1.6
eScan, version 1.2.0
JBC, version 4.1.3
eSlate/DAU, version 4.1.3
VBO, version 1.7.5
eCM Manager, version 1.1.7

Prepared February 25, 2006
By Paul Craft

Scope of Work and Reporting

This report is prepared as a supplement and attachment to the "Staff Review and Analysis" (SOS Report) as prepared by the California Secretary of State's Office of Voting Systems Technology Assessment (OVSTA) on February 24, 2006.

A large part of the consulting work product was providing assistance to OVSTA in both the planning and conduct of voting system tests. The majority of the findings are reported in the SOS Report. This report will be limited to a description of the tasks performed and findings that are not covered in the SOS Report.

Our expertise is in methodologies for examining computerized voting systems, analysis of systems operation, developing measurements of system compliance with established criteria, identification and analysis of system anomalies, and collecting evidence of system characteristics and compliance.

We are not attorneys and do not offer legal advice. We have assisted the California Secretary of State in the collection of facts and evidence that he will use in reaching certification decisions. However, to advise him on the determination of whether the system complies with California's certification requirements would require an interpretation of law. Accordingly we do not provide recommendations or any opinion as to whether the system can be certified. Recommendations to the Secretary for or against certification are within the duties of the OVSTA and are included in their report.

The work that we have performed and our findings are strictly limited to the specific serial numbered hardware elements and specific software elements tested during the examination. An inventory of those items is included as attachment A to this report. The results described in this report should be reliable and repeatable for those specific items. The decision to apply those results to decisions about other items is solely at the discretion of and risk of the Secretary of State and the purchasers of systems. Although attachment A of this report can be used as part of a baseline for reaching conclusions about compliance of other items, users of this report who wish to arrive at such conclusions about compliance of purchased systems or the compliance of a system in use should conduct appropriate acceptance testing or system validation analysis to support those conclusions. If they do not have a high level of well-founded confidence in their ability to conduct acceptance testing or validation analysis, we strongly recommend that they contract for the assistance of someone with the required knowledge and experience.

Findings

With the exception of the eScan units, four of the eSlate units, and specific findings highlighted below the system generally performed to the level expected during testing. With exclusion of the eScan units from the system configuration, thorough acceptance testing by purchasers of the system, and appropriate operating procedures, the system appears to be capable of being used to conduct elections producing accurate results meeting the functional requirements of state and federal law, with appropriate security and user friendly interfaces.

Exceptions where the system did not perform to the level expected were:

- As discussed in detail in the SOS Report, the eScans units presented by the vendor for the volume test experienced a level of errors which would make their use in an election difficult.
- As discussed in detail in the SOS Report, four of the one hundred eSlate units presented by the vendor for the volume test experienced repetitive errors and could not complete the test. The four units failed early in testing and consistently thereafter. Given reasonable acceptance testing by a purchaser the problems with these units would be easily detected so that the units could be rejected and returned to the vendor.
- As discussed in detail in the SOS Report there were seventeen incidents of problems with the VBO printer. All of these could be mitigated in use by a hot swap of the printer. However 13 of the errors were false. While this sensitivity is designed to insure that the voter's ballot will be printed and properly displayed for voter verification, the rate of false errors needs to be reduced.

- The cryptic screen display "Printer error EVBO-101" needs to be replaced with a more intuitive message, like "Printer Paper is Too Low to Continue Voting. Please Call a Poll Worker for Assistance."
- When in the Backup and Reset Window of the Servo application, the "Reset" button has no second chance warning for the user. If the eSlate or JBC connected to the Servo has not been backed up and the backup button in the window is not checked, when the Reset button is clicked the data on the attached eSlate of JBC will be erased without warning. A user who does this by mistake will loose data. That said, the data exists in multiple places and there is no function that would erase all copies at one time. The use procedures need to address this, and we suggest providing a second chance warning or a default setting to always back up data in future releases.
- On the eSlate in the audio ballot, upon entering the audio "Ballot Summary" script the instructions state: "Turn the wheel to hear how you have voted in each contest. If you hear one you want to change, press the enter button. Turn the wheel until you hear your new choice and press enter. Continue turning the wheel until you are returned to the ballot summary page." What really happens when you hear your new choice and press select it, you are automatically returned to the ballot summary page. The audio ballot instruction files can be modified by users. We suggest that the audio file for these instructions be modified to better describe what the voter will experience.
- In the audio ballot instructions the "Cast Ballot" button is described as a "round button on the left". It is not really round and the selection wheel on the right could be identified by some voters as a large round button. This deserves further study to see if it is confusing to voters and if so, how the audio file describing the button should be modified.
- The heading on the voter verified ballot does not print out in the alternative languages. Reading the header is not necessary for the voter to review and verify their choices. If users discover that voters who require alternative languages are disturbed by this it might be appropriate for change in future releases of the system.
- The Curbside voting application will require the entire booth to be taken off line and carried out into the parking lot. Although it is not heavy, it will be cumbersome and will likely require two people to move it. It has a wide footprint and is somewhat top heavy. The booth must be activated while connected to the JBC, disconnected and carried to the parking lot. The booth used for this must be at the end of the line of booths. After the voter votes, the booth must be brought back into the precinct and attached to the JBC for the vote to be recorded and to enable the booth for subsequent voters. It will require one trip to and back from the parking lot for each voter. Jurisdictions should plan for this and arrange the booths in each polling place so as to make this as easy as possible.
- When printing Ballot Proofs, the .pdf print generates new file names going from 1 to 88. After that point, it starts reusing the file names, potentially overwriting the other ballot proof files.

- When a race with a write-in is overvoted on a manually marked MarkSense ballot with both a mark for a candidate and a write-in vote the write-in overrides the overvote condition. The system design assumes the write-in shows voter intent.
- When there is a double write-in on a "vote for two" race, if both candidate names are identical the write-ins are counted as one write-in vote with and one undervote.
- Printed ballots do not have marks which distinguish regular partisan ballots from Decline to State (DTS) ballots. A code on the ballot edge can be used to distinguish the two types of ballots. This contributed to voter/tester confusion and errors in the volume test.
- In the version 6.0 of the system a unique serial number was printed on each ballot and in each bar code. The upgrade to version 6.1 included a change to disable this because California does not allow unique marks or identifiers on ballots. The eScan relies on the unique bar code to insure that no ballot is counted twice. The absence of the unique bar code may make it difficult to resolve eScan ballot jams where the error message is not specific as to whether or not the jammed ballot has been successfully counted or whether it needs to be rescanned.

Summary of System Benchmarking

During the testing in the week of December 12, 2005, the software and firmware applications were loaded from trusted builds. MD5 Check files were created before, at various stages during, and at the end of testing.

On February 1, 2006, because there was no advance in versioning for the Ballot Now, BOSS, Rally, Tally, Servo and eCM Manager applications we ran FileCheck MD5 the check files created at the end of the last round of testing and verified that the installations of the applications and database on the test machines had not been changed since the end of the last round of testing. Additional MD5 Check files were created at the end of testing.

Summary of Security Review

1. User Accounts/Passwords/PINS:
    a. WINNT
        1. User accounts. After initially setting up with an administrator account, we attempted to use an account which was restricted to a Microsoft SuperUser access level and failed. We were told that only a System Administrator login is used by Hart clients and that Hart had not tested for using a lesser account access level. This limits some security practices which may be require the system

administrator use to be restricted. However, the application login accounts support separate levels of access.

2. Passwords. Left for jurisdictions to determine rules.

b. BOSS
   i. User Accounts:
      1. Administrator - Entering the application as an administrator creates a new database automatically. This default database may be replaced later by importing another database.
      2. Update – Able to service the election definition
      3. View – Has strictly an audit view—can not change values.
   ii. Password limits/restrictions. Passwords are set by a prompt at initial entry. There is no initial default. Password restrictions are moderate, requiring a minimum of six characters but not imposing significant complexity rules.

c. Ballot Now
   i. User Accounts: Older documentation lists three levels but this was to be taken out because 'Administrator' is the only login account used. (SuperUser Windows login account did not work).
   ii. The documentation refers to a "Resolute" user account. The Resolute account is limited to viewing the resolution results but can not actual change the ballot.
   iii. Password limits/restrictions. Passwords are set by a prompt at initial entry. There is no initial default. Password restrictions are moderate, requiring a minimum of six characters but not imposing significant complexity rules.

d. eCM. The cryptographic module is invoked within the applications to access and decrypt encrypted data for secure data operations. The module requires its own PIN which requires at least nine upper/lower case letters. The actual encryption key is provided by a USB smart key which must be mounted to perform critical functions..

2. Operating System Setup:
   a. Secure System setups are defined and pre-installed for different modules (BOSS, BallotNow, Tally, Rally).
      i. We walked through the setup but found the documentation was incomplete and inaccurate. The setup for secure operations did a reasonable job of eliminating and disabling unnecessary and risky Windows services and enabling/disabling security features.
      ii. The system required undocumented Registry Key settings. From replies to questions, we received the impression that the procedure for establishing the settings has not been completely defined and validated for this release of the system. While establishing the procedure is highly desirable and commendable, it has the risk of being potential source of problems.

iii. Required special Registry Key settings to meet California rules for protecting privacy of the voter.
iv. The Secure Desktop is only fully implemented while the Tally/Rally applications were active and stops short of secure operating system when applications are closed. It only restricts access when in the application is open and not when users in the desktop environment. Use of encrypted files and signatures reduces this risk but physical security limiting access to the election computers is still required for this and other reasons.

3. Limitations on Test Environment
    a. The AutoVote ballots can only be run in test mode.
    b. Testing was done with computers which were identified as limited in resources. Several minor problems where lockups and system errors occurred were blamed on the limited system resources in the test computers but may not occur in more robust delivered systems.
4. Election Definition. Once a Mobile Ballot Box (MBB) and/or Ballots are generated, the election can not be altered. A change in content or format would require the ballots to be regenerated and reprinted since there is a code on the ballot identifying the specific election definition. The election security intent is commendable but may be expensive if late changes are needed.
5. Logic and Accuracy (LAT) and pre-opening tests.
    a. The Logic and Accuracy tests are set up to use different ballots than the election ballots. They are only run in test mode which keeps a different set of counters for Tally/Ballot Now.
    b. On the eScan, all reports have to be run immediately after the LAT because the test mode reports are lost when the polls open. Except for eScan, a LAT may be run at any time including in the middle of an election day.
    c. The zero reports preceding polls open do not show under votes and over votes which does not allow confirming these values are not pre-set, depending on how they are managed.
6. Physical.
    a. Tamper proof seals on the MBB port door for both the eScan and JBC. During earlier testing, the eScan did not have a door to lock in the MBB but the production model is alleged to have one which can be locked/sealed.
    b. Tamper proof seals or locks are normally recommended for the ballot box to show evidence if the box is opened during voting but the procedures for removing jammed ballots make this impractical.
    c. Tamper proof seals or locks are needed on the eSlate voter verified printer to show evidence of entry if the printer unit is opened.

Attachment A

Hardware Descriptions

The election management system component subsystems consisting of BOSS, Ballot Now, Rally, and Tally may be placed in one or more server/workstations consisting of PC-compatible units supported with appropriate printers and peripherals.

BOSS supports the election definition management and provides support for programming the eSlate PVS. It requires a MBB reader/writer as a peripheral as well as access to printer for various review and audit reports

Ballot Now provides ballot-on-demand service and supports the scanning of the paper ballots. It can use a variety of compatible high speed scanner and laser printer. Ballot Now can be configured in two configurations: Stand-alone or Networked. In the Stand-alone mode, all the Ballot Now processing is done on a single processor. In the Networked configuration, one or more Ballot Now workstations can be attached to the Ballot Now server for multiple resolution workstations and multiple image resolution workstations. In addition to the high-speed scanner, Ballot Now requires access to a PCMCIA reader/writer (to read and write to the MBB) and a large enough hard drive to store the ballot images captured by the scanner.

Rally supports reading the MBBs produced by the JBC and transferring the ballot images, called Cast Voter Records (CVRs) to the Tally subsystem. Rally requires access to a PCMCIA Card Reader/Writer and a connection to the Tally subsystem.

Tally receives all the CSV results from MBBs or from Rally and consolidates the ballot counts for final counting and voting result reporting. Tally requires access to a MBB reader/writer and a printer.

ECM manager is an application that can create, save or copy crypto module tokens and can validate a token.

In the test configuration, these applications were split between two workstations: the BOSS/BallotNow/Tally/ECM workstation and the Rally/SERVO workstation.

eSlate Precinct Voting System

The Precinct Voting System (PVS) consists of a Judge's Booth Controller (JBC) (pictured to the left) connected with an RS485 multipoint cable to 1 to 12 eSlate 3000 DREs. The JBC is operated by the poll worker to configure the DREs, install the election

database, save the CVRs from each of the eSlates connected. When the ballot style (based on precinct or other attributes) and the voter's eligibility has been determined, the poll worker enters the ballot style on the JBC and prints out a slip of paper with a one-time, time-limited access code which the voter then uses to get access to his or her ballot. The JBC and the eSlate are based on a Motorola processor using a proprietary operating system.

Test Configuration for December 12, 2005

Hart InterCivic System 6.0

1. BOSS/Ballot Now/Tally/ECM manager
    a. Dell Optiplex GX 520, Service Tag: 8573T71 Chassis S/N 8573T71
        i. Intel Pentium 4 2.80 GHz processor
        ii. 1016 MByte main memory
        iii. 80 GByte hard drive
        iv. PCMCIA USB Reader Model XI700XA
        v. USB 2.0 Controller
    b. Dell Monitor E771D S/N MX0419T6478011BFH0XZ
    c. HP LaserJet 2420D S/N CN6KC41694
    d. Kodak i260 Scanner S/N 12811222
    e. Application Software Directories
        i. C:\boss
        ii. C:\Program Files\Hart InterCivic
    f. COTS Software
        i. Windows 2000 Professional, Service Pack 5
        ii. Windows Internet Explorer Rel. 6 SP1
        iii. Imaging for Windows Ver. 5.0.2138
        iv. Seagate Software\Report Designer 8.5 and 10.0
        v. Sybase Powerbuilder 6.5.0.444
        vi. Symantec Anti-Virus 8.00
        vii. WinZip 10.0
2. Rally/SERVO
    a. Dell Latitude D600 Service Tag: CYM5241
        i. Intel Pentium M 1.6 GHz processor
        ii. 512 MByte main memory
        iii. 40 GByte hard drive
        iv. USB Hub
        v. PCMCIA Card Slot
    b. Application Software Directories
        i. C:\boss
        ii. C:\Program Files\Hart InterCivic\Rally
        iii. C:\Program Files\Hart InterCivic\SERVO
        iv. C:\Program Files\Hart InterCivic\Shared
    c. COTS Software

i. Windows 2000 Professional, Service Pack 5
ii. Windows Internet Explorer Rel. 6.0 SP 1
iii. Imaging for Windows Ver. 5.0.2138
iv. Seagate Software: 8.5
v. Symantec Anti-Virus 8.00

3. ECM Key (Spyrus Crypto Module USB device)
4. Precinct Voting System 6.0
   a. Judge's Booth Controller 1000B S/N:C02484
   b. eSlate 3000, S/N: A07C5D FW 4.0.16
   c. vBox (VVPAT Printer and Compartment) S/N MT1005000132
   d. DAU 5000 (Interface card for eSlate) S/N B00049
   e. eSlate 3000, S/N: A0008A FW 4.0.16
   f. vBox S/N MT1005000007
   g. DAU 5000 S/N B00023
   h. eSlate 3000, S/N: A05F80 FW 4.0.16
   i. vBox S/N MT1005000109
   j. DAU 5000, S/N: B015E2
   k. eScan Unit S/N G77801 S/W 1.1.6
   l. eScan Ballot Tub
5. Hart InterCivic System 6.0
   a. Directories:
      i. C:\Boss
      ii. C:\Program Files\Hart InterCivic\
         1) Ballot Now
         2) \Rally
         3) \SERVO
         4) \Shared\(Sybase SQL Anywhere)
         5) \Tally
      iii. C:\Program Files\Seagate Software
      iv. C:\WINNT
         1) \Crystal
         2) \PIXTRAN
         3) \System32\(32 added/replaced files)

Test Configuration for February 1, 2006

Hart InterCivic System 6.1

Version 6.1 differs from version 6.0 as follows:

- JBC, firmware increased from version 4.0.16 to version 4.1.3.
- eSlate/DAU firmware increased from version 4.0.16 to version 4.1.3
- eScan firmware increased from version 1.1.6 to version 1.1.0

1. BOSS/Ballot Now/Tally/ECM manager
    a. Dell Optiplex GX 520, Service Tag: 8573T71 Chassis S/N 8573T71
        i. Intel Pentium 4 2.80 GHz processor
        ii. 1016 MByte main memory
        iii. 80 GByte hard drive
        iv. PCMCIA USB Reader Model XI700XA
        v. USB 2.0 Controller
    b. Dell Monitor E771D S/N MY0X378247603464BETU
    c. HP LaserJet 2420D S/N CNGKC41694
    d. Kodak i260 Scanner S/N 12811221
    e. Application Software Directories
        i. C:\boss
        ii. C:\Program Files\Hart InterCivic
    f. COTS Software
        i. Windows 2000 Professional, Service Pack 5
        ii. Windows Internet Explorer Rel. 6 SP1
        iii. Imaging for Windows Ver. 5.0.2138
        iv. Seagate Software\Report Designer 8.5 and 10.0
        v. Sybase Powerbuilder 6.5.0.444
        vi. Symantec Anti-Virus 8.00
        vii. WinZip 10.0
2. Rally/SERVO
    a. Dell Latitude D600 Service Tag: CYM5241
        i. Intel Pentium M 1.6 GHz processor
        ii. 512 MByte main memory
        iii. 40 GByte hard drive
        iv. USB Hub
        v. PCMCIA Card Slot
    b. Application Software Directories
        i. C:\boss
        ii. C:\Program Files\Hart InterCivic\Rally
        iii. C:\Program Files\Hart InterCivic\SERVO
        iv. C:\Program Files\Hart InterCivic\Shared
    c. COTS Software
        i. Windows 2000 Professional, Service Pack 5
        ii. Windows Internet Explorer Rel. 6.0 SP 1
        iii. Imaging for Windows Ver. 5.0.2138
        iv. Seagate Software: 8.5
        v. Symantec Anti-Virus 8.00
3. ECM Key (Spyrus Crypto Module USB device)
4. Precinct Voting System 6.1
    a. Judge's Booth Controller JBC1000B S/N:C0011B FW 4.1.3
    b. eSlate 3000, S/N: A07C5D FW 4.1.3

c. vBox (VVPAT Printer and Compartment) S/N MT1005000115 FW 1.7.5
d. DAU 5000 (Interface card for eSlate) S/N B00049
e. eSlate 3000, S/N: A0504B FW 4.1.3
f. vBox S/N MT1005000010 FW1.7.5
g. DAU 5000 S/N B00E7D
h. eScan Unit S/N G77825 S/W 1.2.0
i. eScan Ballot Tub

5. Hart InterCivic System 6.0
    a. Directories:
        i. C:\Boss
        ii. C:\Program Files\Hart InterCivic\
            1. Ballot Now
            2. \Rally
            3. \SERVO
            4. \Shared\(Sybase SQL Anywhere)
            5. \Tally
        iii. C:\Program Files\Seagate Software
        iv. C:\WINNT
            1. \Crystal
            2. \PIXTRAN
            3. \System32\(32 added/replaced files)